International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876
Impact Factor: RJIF 5.44
www.newengineeringjournal.in
Volume 4; Issue 1; January 2018; Page No. 25-31

Multimodal biometric system: A review

Waleed Dahea[1], HS Fadewar[2]
[1] Research Scholar, School of Computational Sciences, SRTM University, Nanded, Maharashtra, India
[1] Computer Science and Information Technology, Thamar University, Dhamar, Yemen
[2] Assistant Professor, School of Computational Sciences, SRTM University, Nanded, Maharashtra, India

Abstract
The procedure by which a person's identity can be authenticated by applying the physical or behavioral trait is called Biometric. Physical traits, similar to fingerprints, face, iris and so on depend on physical characteristics which are by and large inborn and stable. Behavioral traits, similar to voice, signature or keystroke and so on then again, is a quantifiable characteristic. That is acquired after some time and is liable to think change. Unimodal biometric systems created for each of these biometric features may not generally meet the required performance. The techniques are broke down to incorporate the different features together to obtain a multimodal biometric system. The current research uncovers that multimodal biometric system is more viable in authentication. The goal of this paper is to highlight the significance of the utilization of multimodal biometrics in the area of secure individual confirmation. This paper gives an alternate discernment to utilize biometrics as a largest amount of system security with the combination of numerous biometric modalities.

Keywords: biometrics, unimodal biometrics, multimodal biometric system, fusion levels

1. Introduction
A biometric system measures at least one physical or behavioral attributes including unique fingerprint, palm print, face, iris, retina, ear, voice, signature, gait, hand-vein data of an individual to decide or check his identity. These qualities are alluded by various terms, for example, traits, indicators, identifiers, or modalities [1]. A Biometric system is an identification system in view of the utilization of various biometric features of people by the investigation of physiological characteristics, for example, fingerprints, eye retinas and irises, voice designs, facial examples and hand estimations for authentication purposes or behavioral attributes. authentication systems setup with one biometric modality may not be adequate for the related application as far as properties, for example, universality, distinctiveness, acceptability etc. Unimodal biometric systems are missing operational favorable circumstances relating to the performance and accuracy [2]. 100% accuracy may not accomplish in unimodal systems by virtue of the limitations, for example, the noise in the sensor data, intra-class variations, inter-class similarities, lack of universality, interoperability issues, spoof attacks and other vulnerabilities. Accuracy in biometrics is measured in terms of 'error rates'. The two mostly utilized error rates are False Acceptance Rate (FAR) and False Rejection Rate (FRR). Multimodal biometric system is a refined arrangement of unimodal system fusing the therapeutic measures for the downsides looked in unimodal biometric system.

2. Attacks on Biometric Systems
Even though biometric systems offer several advantages over traditional token (e.g. key) or knowledge (e.g. password) based authentication schemes. They are still vulnerable to attacks. These attacks can be classified into eight classes.

Class I: Spoof attack: In this type of attack a fake biometric e.g. (finger made from silicon, face mask, lens including iris texture) can be presented to a sensor.

Class II: replay attack. In it an intersected biometric data is submitted to the feature extractor by passing the sensor. To detect the replay attack, the authenticator as to ensure that the data is captured through the sensor and has not been injected. But sensor noise and input variations make hurdle in this detection so the best method is either to build a time stamp or using challenge and response mechanism to address the replay attack.

Class III: Substitution attack: In the third type of attack the feature exactor module is replaced by a Trojan horse program that functions according to its designer specifications. Then the attacker gets an access to storage either locally or globally. He can overwrite the legitimate users template with his /her own –in essence stealing their identity.

Class IV: In the fourth type of attack a genuine feature values are replaced with values (synthetic or real) selected by the attacker or an imposter.

Class V: In this type of attack the matcher is replaced with a Trojan horse program. This class of attack is called Trojan horse Attack.

Class VI: This type of attack occurs on the template database.

The template database can be added, modified or removed. The templates can also be stolen which can be most dangerous.

Class VII: Transmission attack: A man in the middle attack is possible while the data is transmitted from one component to another. The attacker can manipulate the input data stream, send a fake template as an enrolled user, inject an artificial matching score or even generate a forged response.

Class VIII: Lastly the matured result (accept or reject) can be overridden by the attacker.

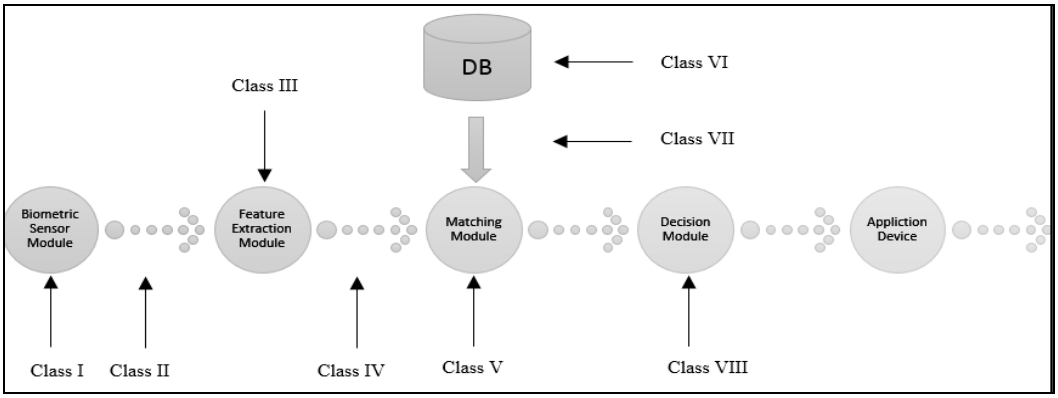

Fig 1: Location of attacks in Biometric System

3. Unimodal System Problems

In the real world, unimodal is used in Biometric systems applications. They depend on the evidence of a one source of information for authentication. These systems have to deal with variety of problems such as: *Noise* in the sensed data. (e.g., due to repeated use of fingerprint sensor) *Intra-class* variation: User who is incorrectly acting with the sensor typically causes these variations. *Inter-class similarities*: In a Biometric System where there are large no of users, there may be inter–class overlap in the feature space of multiple users. *Non-Universality*: The Biometric System might not be able to acquire a meaningful Biometric data from a subset of users. *Spoof Attack*: This attack occurs when signature or voice are used in Biometric System. Not all but some of the limitations of the unimodal can be overcome by including multiple source of information for identification. These types of system are called as Multimodal Biometric Systems. These systems are more reliable due to the presence of multiple, independent biometrics. They also have better performance, as it would be difficult for an imposter to spoof multiple biometric traits of a genuine user simultaneously. Moreover, they provide a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a „live" user is indeed present at the point of data acquisition. Some common multimodal biometrics are: face and fingerprint, face and iris, iris and fingerprint etc.

4. Multimodal Biometric System

Multimodal biometric is a system that consolidates the obtained result from more than one biometric traits for the purpose of individual identification. Multimodal biometric systems are more reliable than unimodal because many independent biometric modalities are used. The use of multimodal biometric system may result high accurate and secure biometric identification system, as unimodal biometric system may not provide high accurate identification due to non-universality. Such as, a few proportions of individuals can have cut, worn or unrecognizable prints, fingerprint biometric may produce improper results. The failure in Multimodal biometric Systems of any one technology may not influence seriously the individual identification as different technologies can be successfully employed. Hence the spoofing can extremely be minimized; thus improving the efficiency of the overall system. The reduction in failure to enroll (FTE) rate in multimodal biometric system is very significant and which is one of main advantages of this system. The four common modules in any biometric system are [3] - sensor module, feature extraction module, matching module and decision making module. Each of these modules is described below.

4.1 Sensor Module

In this module, the raw data of the user is measured by using the biometric sensor or scanner. This raw biometric data is recorded and then it is transferred to the next module for feature extraction. The various factors like cost and size are impacted by the design of the sensor module of the biometric system.

4.2 Feature Extraction Module

In this module, the raw data that transferred from the sensor module. Thus generating a synoptic but indicative digital representation of the underlying traits or modalities. After extracting the features it is given as input to the matching module for further comparison.

4.3 Matching Module

The extracted features when compared with the templates in the database generate a match score. This match score may be controlled by the quality of the given biometric data. The matching module also condensed a decision making module in which the generated match score is used to validate the claimed identity.

4.4 Decision Making Module

Decision making module identifies whether the user is a genuine user or an impostor based on the match scores. These

are used to either validate the identity of a person or provides a ranking of the enrolled identities for identifying an individual. A simple block diagram for multimodal biometric system is shown in Figure-2.

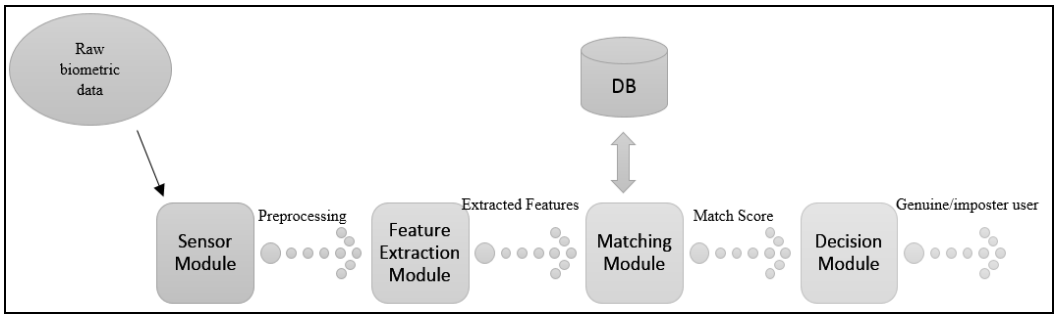

Fig 2: Block diagram of biometric system

5. Levels of Fusion

The information of the multimodal system can be fused at any of the four modules:

Fusion at the sensor level: In this the raw data from different sensors are fused. In it we can either use samples of same biometric trait obtained from multiple compatible sensors or multiple instances of same biometric trait obtained using a single sensor. In it the data is fused at very early stage so it has a lot of information as compared to other fusion levels. Very less work has been done in this area.
Figure-3 shows the fusion at Sensor level.

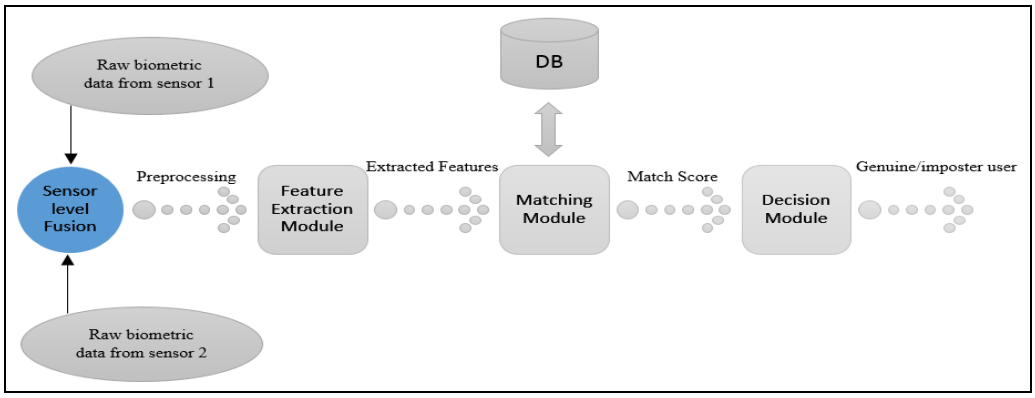

Fig 3: Sensor level Fusion

Fusion at the Feature Extraction Level

The data or the feature set originating from multiple sensors or sources are fused together. Features extracted from each sensor form a feature vector. These features vectors are then concatenated to form a single new vector. In feature level fusion, the same feature extraction algorithm or another feature extraction algorithm on multiple modalities can be used for that features has to be fused. The feature level fusion is challenging because relationship between features is not known and structurally incompatible features are common and the curse of dimensionality. Because of these difficulties, only limited work is reported on feature level fusion of multimodal biometric system. Feature level fusion shown in Figure – 4

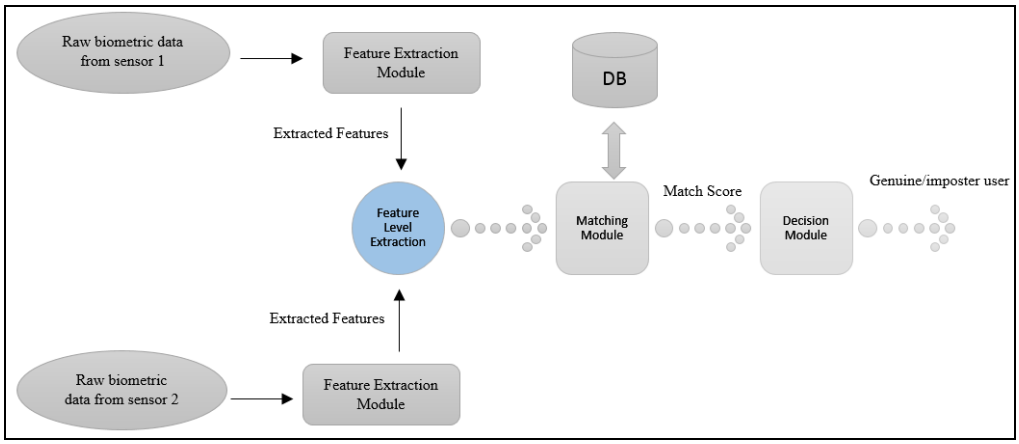

Fig4: Feature level fusion

Fusion at Matcher Score Level

Each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. The scores that obtained from different matchers are not identical, score normalization technique is adapted to map the scores obtained from different matchers on to a same range. These scores contain the wealthy information about the input. Also it is quite easy to combine the scores of different biometrics so lot of work has been done in this field. Matching score level fusion shown in Figure-5.

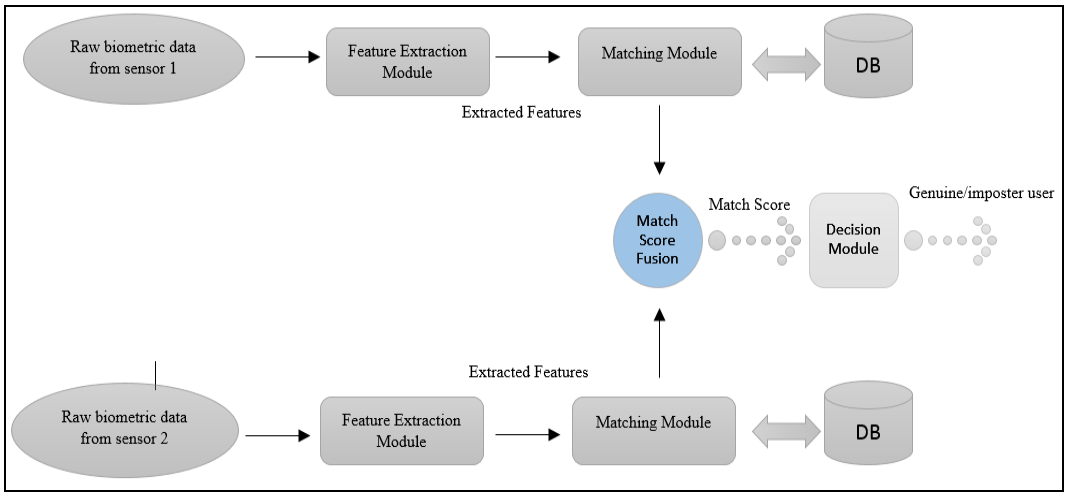

Fig 5: Matching Score Level Fusion

Fusion at the Decision Level

The final outputs of the multiple classifiers are combined. A majority vote scheme can be used to make final decision. Decision level fusion includes very abstract level of information so they are less preferred in designing multimodal biometric systems. Biometric systems that integrate information at the early stages are more effective than those in which integration is done in later stages. So fusion at the feature level is expected to give better recognition results but it is difficult to integrate at this level because feature sets of the various systems may not be compatible. More over all commercial Biometric systems don't provide access to the feature sets, which they use in their products. Fusion at the matcher score level is usually preferred because it is relatively easy to access and combine the scores presented by different modalities. Decision level fusion as shown in Figure-5

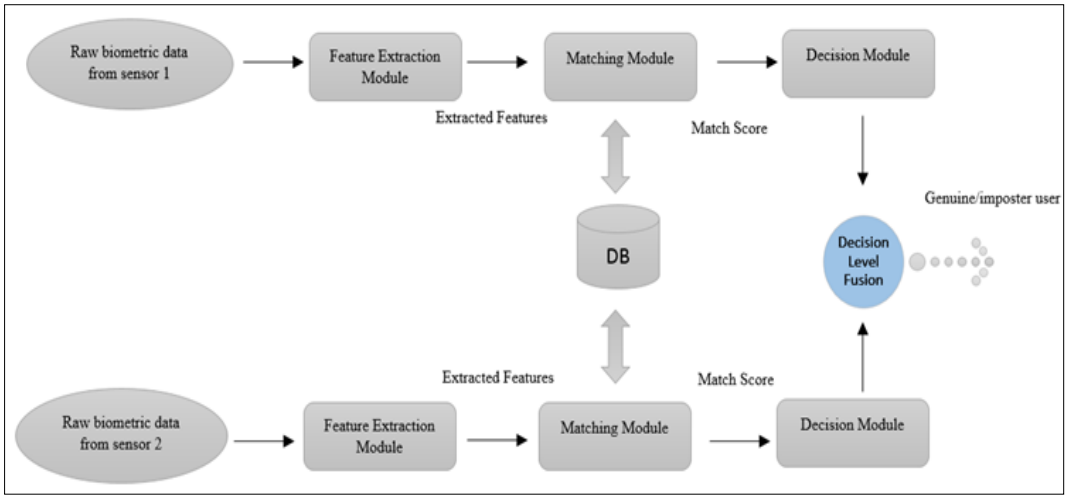

Fig 6: Decision level fusion

6. Comparison of Varoius Biometric Technologies

Individual qualities of a physical or a behavioral trait fulfilling the seven properties like Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability, and Circumvention also go around could be termed Likewise as a biometric [8]. *Universality* means every individual should have the biometric trait. *Distinctiveness* ensures that no two individuals should be identical in terms of the biometric traits. *Permanence* means the biometric trait of an individual should be sufficiently invariant over a period of time. *Collectability (measurability)* means it should be easily measurable without any inconvenience to the user. *Performance* relates to accuracy, speed of the technology used. *Acceptability* means the user acceptance without objection to the collection of the

biometric and *Circumvention* relates to the ease with which the biometric trait can be deceived. Brief comparisons of the different biometric identifier in terms of those seven features are shown in the Table-1**.**

Table 1: Comparison of different biometric technologies

Biometric identifier / **Characteristics**	**Finger**	**Facial**	**Iris**	**Hand**	**Retina**	**Signature**
Universality	high	high	high	mid	high	low
Distinctiveness	high	low	high	mid	high	low
Permanence	high	mid	high	mid	mid	low
Collectability	mid	high	mid	high	low	high
Performance	high	low	high	mid	high	low
Acceptability	high	high	low	mid	low	high
Circumvention	mid	high	low	mid	low	high

In the Table-1 'high' indicates that the particular biometric identifier is having very good performance, whereas poor performance in the evaluation criteria is represented by 'low' and average performance in the evaluation criteria is represented by 'mid'. From the Table-1 it is evident that for every biometric trait have merits and demerits in each of the seven characteristics. Hence on account of the above limitations it is better to use more than one biometric identifier.

Table 2: Strength and Weakness of different Biometric Identities

Biometric-Identifier	**Strengths**	**Weakness**
Finger- scan	High level of accuracy, easy to use, flexibility	Performance can deteriorate over time, unable to enroll some percentage of users
Facial- scan	Able to operate without user cooperation	Changes in physiological characteristic reduce matching accuracy
Signature- scan	Resistant to imposters	Lead to increased error rates
Hand- scan	Reliable core technology, stable physiological characteristic.	Limited accuracy
Retina- scan	Highly accurate	Difficult to use and capture
Iris-scan	Resistance to false matching	Difficult of use and capture

The strength and weakness of different biometric identities [7] are also listed in the Table-2. Hence the selection of combination of biometric identity can be made easy by the perusal of the given table, which in turn helps to develop an accurate and high performance biometric identification as well as authentication.

7. Related Work

The unimodal biometric system is most widely used in various applications. On account of the limitations raised by the unimodal biometric system many users resorted to multimodal biometric system in order to provide maximum level of accurate authentication [8]. Effective utilization of the advantages of multiple biometric traits is applied to enhance the performance in many aspects including accuracy, noise resistance, and universality, spoof attacks, and reduce performance degradation in huge database applications. Nowadays, new algorithms and applications of multi-modal biometrics are emerging tremendously. The most commonly used biometrics is face, that is, either as a single trait or combined with other trait as multi-modal biometrics. Face combined with other biometrics at different levels of fusion.

Besbes *et al*. [9] proposed a multi-modal biometric system which enhanced recognition accuracy and population coverage by using iris and fingerprint. Shahin *et al*. [10] proposed a high security system by fusing hand veins, hand geometry and fingerprint. Kumar and Ravikanth [11] proposed an approach for personal authentication using both finger geometry and dorsal finger knuckle surface features provides a high performance in person authentication. Chandran *et al*. [12] investigated and proposed a method to improve the performance by combining iris and fingerprint. Chin *et al*. [13] proposed a method at feature level which integrate palm print and fingerprint and a series of preprocessing steps are applied on palm and finger print to increase efficiency and for feature extraction of 2D by using Gabor filter at feature level. Sheetal Chaudhary and Rajender Nath proposed a system by integrating palmprint, fingerprint and face based on score level fusion [14].

Fan Yang and Baofeng Ma proposed a method to establish an identity by combining different modalities like fingerprint, hand geometry, palm print using feature and match score fusion [15]. Muhammad Imran Razzak *et al*. [16] proposed a multi-modal recognition system using the biometric traits like face and finger vein. This system effectively reducing the error rates like FAR (False Acceptance Rate) and improving GAR (Genuine

Acceptance Rate). Table-3 shows the individual results of various works using multi-modal systems that have been implemented and deployed, using different fusion levels and different algorithms [17].

Table 3: Different interpretations of quality in biometrics from literature

Year	Author	Modality Fused	Level of Fusion	Interpretation
2012	Hariprasath, S, Prabakar, T.N,	Iris and palm print [18]	Fusion at score level fusion	Gives high accuracy
2011	N. Gargouri Ben Ayed, A. D. Masmoudi and D. S. Masmoudi	Fingerprint and face [19]	Fusion done at score match- level with sum weighted method	Excellent method giving higher performance
2010	P. K. Mahesh and M. N. S. Swamy	Voice and palm print [20]	Fusion at score matching level	Accuracy is 98% and error rates are reduced
2010	M. Hanmandlu, A. Kumar and V. K. Madasu	Using combinations of various modalities [21]	Fusion at score matching level	Higher accuracy in score level than decision level
2010	A. Yazdanpanah, K. Faez and R. Amirfattahi	Face, Ear and Gait [22]	Fusion at score matching level	Higher accuracy
2009	D. Kisku, A. Rattani, P. Gupta and J. Sing	Face & Palm- print [23]	Fusion at low level	Makes system more robust.
2010	Zhu Le-qing, Zhang San-yuan	Finger-print, knuckle-print and palm- print [24]	Fusion at Feature level	Improved matching accuracy and searching efficiency
2012	Yeong Gon Kim, Kwang Yong Shin	Face and both irises [25]	Fusion at Score level	Better performance by using Support Vector Machine.

From the literature survey it is inferred that the different fusion levels and combinations of different biometric modalities are being fused by different researchers are for accurate personal identification. Also the performance metrics used for quality-based multi-modal biometric system, fusion approaches must be carefully selected as the precision in personal identification or verification rate may be affected. All performance metrics are not made applicable for all the four fusion levels. There is a scope for better evaluation framework for biometric quality assessment metrics by correlating with the available fusion schemes. Also computational cost in the development of quality assessment approach shall be reduced.

8. Types of Multimodal Systems

Based on the traits, sensors and feature sets many different types of multimodal systems are there:

- Single biometric trait, multiple sensors: Multiple sensors are used to record the same biometric characteristic. The raw data taken from different sensors can then be combined at the feature level or matcher score level to improve the performance of the system.
- Multiple biometrics: Multiple biometric traits such as fingerprints and face can be combined. Different sensors are used for each biometric characteristic. The interdependency of the traits ensures a significant improvement in the performance of the system. A commercial product BioID [26] uses voice, lip motion and face of a user to verify identity.
- Multiple units, single biometric traits: Two or more fingers of a single user can be used as a biometric trait. It is inexpensive way of improving system performance, as it doesn't require multiple sensors or incorporating additional feature extraction or matching modules. Iris can also be included in this category.
- Multiple snapshots of single biometric: In this more than one instance of the same biometric is used for the recognition. For e.g. multiple impressions of the same finger or multiple samples of the voice. Multiple matching algorithms for the same biometric: In it different methods can be applied to feature extraction and matching of the biometric characteristic.

9. Modes of Operation

A multimodal biometric system can work in three modes:

- **Serial mode:** In the serial mode the output of one biometric characteristic is used to reduce the no of possible identities before the next characteristic is used. So multiple source of information is not collected simultaneously.
- **Parallel mode**: In it the information from multiple characteristics is taken together to perform recognition.
- **Hierarchical mode:** In it individual classifiers are combined in a tree like structure. This mode is well suited where we have large no of classifiers.

10. Design Issues in Multibiometrics

- Choice and number of biometric indicators.
- Fusion Level:
- Representation (incompatibility & unavailability of features).
- Matching score (preferred; normalize matching scores).
- Decision (too rigid; majority vote).
- Fusion methodology.
- Learning weights of individual biometric for each user.
- Cost versus performance trade-off.
- Verification vs. Identification system.

11. Applications of Multimodal Biometrics

The defense and the intelligence communities require high level security systems. Border management, interface for criminal and civil applications, and first responder verification are the major areas which use the Multimodal Biometrics. Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. Multi modal biometrics can provide best solutions to all the areas where high level security systems are needed.

12. Conclusions

There are many multimodal biometric systems in practice for authentication of an individual, choice of appropriate modal, select of optimal fusion level and redundancy in the extracted features are still some of the shortcomings faced in the design of multimodal biometric system that needs to be addressed.

The different approaches that are possible in multimodal biometric systems, the suitable fusion levels, and the integration strategies that can be chosen to consolidate information were discussed here. The combination of more than one biometrics can apply to enhance the security. Performance and the advanced security level made the multimodal biometric systems popular in these days. The high accuracy may be achieved by using different methods for feature selection scheme to reduce the dimensionality, for example, genetic algorithms.

13. References

1. Jain AK, Arun A Ross, Karthik Nandakumar. Introduction to Biometrics, Foreword by James Wayman, Springer, ISBN 978- 0-387-77325-4.
2. Sasidhar K, Vijaya L Kakulapati *et al*. Multimodal Biometric Systems –STUDY To Improve Accuracy And Performance, IJCSES, 2010, 1(2).
3. Sanjekar PS, Patil JB. An Overview of Multimodal Biometrics, Signal & Image Processing: An International Journal (SIPIJ), 2013, 4(1).
4. Ross A, Govindarajan R. Feature level fusion using hand and face biometrics, Proc of SPIE Conference on Biometric Technology for Human Identification. 2005; 5779:196-204.
5. Mini Singh Ahuja, Sumit Chabbra, A Survey of Multimodal Biometrics, International journal of Computer Science and its Applications, [ISSN 2250 – 3765].
6. Jain AK, Ross A, Prabhakar S. An Introduction to Biometric Recognition, IEEE Trans. on Circuits and Systems for Video Technology. 2004; 14(1):4-19.
7. Samir Nanavati, Michael Thieme, Raj Nanavati. Biometrics Identity Verification in a Networked World, A Wiley Tech Brief, Wiley Computer publishing, ISBN-0471-09945-7.
8. Soyuj Kumar Sahoo, Tarun Choubisa, Mahadeva Prasanna SR. Multimodal Biometric Person Authentication: A Review IETE Technical Review, 2012, 29(1).
9. Besbes F, Trichili H, Solaiman B. Multimodal Biometric System Based on Fingerprint Identification and Iris Recognition Information and Communication Technologies: From Theory to Applications, ICTTA 3rd International Conference, 2008.
10. Shahin MK, Badawi AM, Rasmy ME. A Multimodal Hand Vein,Hand Geometry and Fingerprint Prototype design for High Security Biometrics, CIBEC'08, 2008.
11. Kumar A, Ravikanth C. Personal Authentication Using Finger Knuckle Surface, Information Forensics and Security, IEEE Transactions on, 2009, 4(1).
12. Chandran GC, Rajesh RS. Performance Analysis of Multimodal Biometric System Authentication, Int. J Computer. Sci. Network Security. 2009; 9:3.
13. Chin YJ, Ong TS, Goh MKO, Hiew BY. Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security, 2009.
14. Sheetal Chaudhary, Rajender Nath. A Multimodal Biometric Recognition System Based on Fusion of Palmprint, Fingerprint and Face. International Conference on Advances in Recent Technologies in Communication and Computing. 978-0-7695-3845-7/ 2009 IEEE.
15. Fan Yang, Baofeng Ma. A New Mixed Mode Biometrics Information Fusion on Fingerprint, Hand-geometry and Palm Print. 4th international Conference on Image and Graphics. 7695-2929-1/07 IEEE.
16. Muhammad Imran Razzak, Muhammad Khurram Khan, *et al*. Multimodal Biometric Recognition Based On Fusion Of Low Resolution Face And Finger Veins, ICIC International ISSN 1349-4198, 2011, 4679-4689.
17. Sanjekar PS, Patil JB. An Overview of Multimodal Biometrics, Signal & Image Processing: An International Journal (SIPIJ), 2013, 4(1).
18. Hariprasath S, Prabakar TN. Multimodal biometric recognition using iris feature extraction and palmprint features, Advances in Engineering Science and Management (ICAESM), International Conference on, 2012.
19. Gargouri Ben Ayed N, Masmoudi AD, Masmoudi DS. A New Human Identification based on Fusion Fingerprints and Faces Biometrics using LBP and GWN Descriptors, in Proc. of 8th International Multi-Conference on Systems, Signals and Devices (SSD), Sousse. 2011; 1(7):22-25.
20. Mahesh PK, Swamy MNS. A Biometric Identification System based on the Fusion of Palmprint and Speech Signal, in Proc. of International Conference on Signal and Image Processing (ICSIP), Chennai. 2010; 186(190):15-17.
21. Hanmandlu M, Kumar A, Madasu VK. Fusion of Hand Based Biometrics using Particle Swarm optimization, in Proc. Fifth International Conference on Information Technology: New Generations (ITNG), 2010, 783-788.
22. Yazdanpanah A, Faez K, Amirfattahi R. Multimodal Biometric System using Face, Ear and Gait Biometrics, in Proc. of 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA), Kuala Lumpur. 2010; 251(254):10-13.
23. Kisku D, Rattani A, Gupta P, Sing J. Biometric Sensor Image Fusion for Identity Verification: A Case Study with Wavelet-Based Fusion Rules Graph Matching, in Proc. of IEEE Conference on Technologies for Homeland Security, HST '09, Boston. 2009; 433(439):11-12.
24. Zhu Le-qing, Zhang San-yuan. Multimodal biometric identification system based on finger geometry, knuckle print and palm print, Pattern Recognition Letters. 2010; 31:1641-1649.
25. Yeong Gon Kim, Kwang Yong Shin, *et al*., Multimodal Biometric System Based on theRecognition of Face and Both Irises, International Journal of Advanced Robotic Systems, 2012.
26. Frischholz R, Dieckmann U. BiolD: A multimodal biometric identification system, Computer. 2000; 33(2):64-68.
27. Sheena S, Sheena M. A study of multimodal biometric system. International Journal of Research in Engineering and Technology, ISSN, 2014, 2321-7308.